Claims

What is claimed is:

[c1] A network system providing integration, comprising:

a client computer;

a server;

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function.

[c2] The network system of claim 1, further comprising:

a security device holding authentication information; and

a card reader attached to the client computer for reading the security device.

[c3] The network system of claim 2, wherein a certificate is stored on the security device.

[c4] The network system of claim 2, wherein the security device is a smart card.

[c5] The network system of claim 1, further comprising:

a directory service accessed by the server-side cryptographic function.

[c6] The network system of claim 5, wherein the directory service is lightweight directory access protocol compliant.

[c7] The network system of claim 1, wherein the client-side cryptographic function and the server-side cryptographic function employ the same cryptographic scheme.

[c8] The network system of claim 1, wherein the server-side cryptographic function uses a random number generator to generate a challenge string.

[c9] The network system of claim 1, wherein a client-side cryptographic function uses a random number generator to generate a response string.

[c10] The network system of claim 1, wherein the client-side cryptographic function generates a signed response string.

[c11] The network system of claim 1, wherein the server-side cryptographic function generates a challenge string.

[c12] The network system of claim 1, wherein the server-side cryptographic function verifies the signed response string.

[c13] The network system of claim 1, wherein the dial-up client operates in terminal mode.

[c14] A network system providing integration, comprising:

a client computer;

a server;

a server-side cryptographic function providing cryptographic services located on the server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

a security device holding authentication information;

a card reader attached to the client computer for reading the security device; and

a directory service accessed by the server-side cryptographic function.

[c15] A client computer comprising:

a dial-up client providing dialing services to the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function.

[c16] The client computer of claim 15, further comprising:

a card reader attached to the client computer for reading a security device.

[c17] The client computer of claim 15, wherein a security device is a smart card.

[c18] The client computer of claim 15, wherein the dial-up client comprises a SDLogin component and a SDSetupDial component.

[c19] The client computer of claim 15, wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode.